This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the
original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS

- TEXT CUT OFF AT TOP, BOTTOM OR SIDES

- FADED TEXT

- ILLEGIBLE TEXT

- SKEWED/SLANTED IMAGES

- COLORED PHOTOS

- BLACK OR VERY BLACK AND WHITE DARK PHOTOS

- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: CRYPTOGRAPHIC METHOD AND APPARATUS WITH ELECTRONICALLY REDEFINABLE ALGORITHM

(57) Abstract

A cryptographic apparatus (10) for encrypting and decrypting digital words includes a mechanism that permits a cipher algorithm to be electronically stored after the manufacture of the apparatus. The storing mechanism includes at least one electrically erasable, programmable gate array (34, 36) containing a portion of the cipher algorithm and at least one random access memory device (32) coupled to the array for storing digital data generated by the algorithm. A mechanism (12) which is coupled to the gate array and memory device controls the execution of the algorithm for each digital word thereby decrypting encrypted digital words and encrypting non-encrypted digital words.

-1-

5

CRYPTOGRAPHIC METHOD AND APPARATUS WITH
ELECTRONICALLY REDEFINABLE ALGORITHM

10

Background of the Invention

This invention is generally directed to the field of
digital cryptographic devices and is more specifically
15 directed to the architecture and method by which a cipher
algorithm is stored in the cryptographic apparatus. This
invention also addresses a method for manufacturing
encrypted communications equipment in an unsecured
environment as a result of the cipher algorithm being
20 loaded into the encryption device after the manufacture
of the equipment.

In a typical encryption device, a secret key is
utilized in conjunction with a cipher algorithm to
encrypt and decrypt messages. The keys may be changed as
25 frequently as desired in order to enhance security.

The cipher algorithm which consists of the steps by
which the message is encrypted and decrypted using a
particular key is frequently protected in order to
maintain high levels of security. If the algorithm is
30 known, it becomes easier to decipher a coded message
since only the message and key are then unknowns. Thus
it is important that the algorithm itself be protected
for maximum security applications.

35

- 2 -

It is also important that the electronic circuits in which the algorithm resides be designed not to fail in a way which would compromise the message being communicated. Algorithms which are stored in logic hardware are easier to be made to "fail safe" than algorithms stored in software. The manufacture of logic hardware containing the cipher algorithms and equipment containing same is often strictly controlled. The manufacture of communications equipment containing such fixed encryption logic requires substantial additional procedures as compared with communications equipment that does not utilize encryption. This results in the need for strict controls and substantially increases manufacturing costs.

Objects of the Invention

It is an object of the present invention to provide an encryption apparatus having an architecture which permits the cipher algorithm to be electronically entered subsequent to the manufacture of the apparatus and subsequent to the manufacture of communications equipment utilizing the encryption apparatus.

Another object of this invention is to provide an improved method for the manufacture of encrypted communications equipment in which security control measures need not be utilized during the manufacture of such equipment.

Brief Description of the Drawings

Figure 1 is a block diagram of an embodiment of an encryption device according to the present invention.

Figure 2 is a block diagram of communications equipment incorporating the encryption apparatus in accordance with the present invention.

Detailed Description

        Figure 1 illustrates an embodiment 10 of a
    cryptographic apparatus in which the cipher algorithm can
 5 be electronically defined after its manufacture in
    accordance with the present invention. A sequence
    controller 12 shown to the left of the dashed line
    includes a program counter 14 having an output coupled by
    bus 16 to multiplexer 18. The output of multiplexer 18
10 is coupled to an electronically erasable, programmable
    array logic device (EEPAL) 20. Such EEPAL devices are
    commercially available and consist of a number of logic
    gates which can be electronically programmed to
    interconnect to each other to produce an output
15 determined by a Boolean algebraic formula operating on
    the input data. As used herein, array logic devices do
    not include microprocessors. It is important that the
    array logic devices be electronically programmable and
    are preferably erasable to permit reprogramming. The
20 output of device 20 is coupled by latch 22 to buffer 24
    and to latch 26. An output of device 20 also provides a
    clock input to program counter 14 which causes the
    counter to increment periodically and step through a
    preprogrammed number of steps.
25   The general purpose of sequence controller 12 is to
    control the cyclic operation sequence of the remainder of
    the circuitry shown in Figure 1, i.e. implement the
    cipher algorithm on a step by step basis. A common
    address bus 28 with communication port 29 and a data bus
30 30 with communication port 31 establish digital
    communication paths with EEPAL 20, random access memory
    (RAM) device 32, and EEPAL's 34 and 36. RAM 32 is
    addressed by multiplexer 38 which selects between the
    output 16 of program counter 14 or address bus 28. Data
35 is input to RAM 32 by data bus 30. The data information
    stored in a particular address is coupled from RAM 32 by
    latch 40 and buffer 42 to data bus 30.

EEPAL 34 has address and data inputs from the respective buses. The output from EEPAL 34 is coupled by latch 44 and buffer 46 to data bus 30. Similarly, EEPAL 36 receives address and data inputs from the respective

5   bus lines. Its output as determined by its particular gate configuration is coupled to data bus 30 by latch 48 and buffer 50. Its output is also coupled to latch 26 and defines the encrypted digital output 52 at the end of the program sequence which is communicated to latch 26

10 via the output of latch 22.

The digital information to be encrypted is coupled by input 54 to buffer 56 which in turn couples the information to data bus 30. The digital information consists of digital words having one or more bits. It

15 will be understood that the encryption of the input data by the encryption apparatus 10 must be accomplished prior to the input of the next information to be encrypted in order to maintain a real time message flow. Thus it will be apparent that the clock (not shown) which provides

20 clock information to the elements shown in Figure 1 must be of a sufficient rate to allow the number of steps required by the cipher algorithm to be completed within the input time frame.

One important aspect of the present invention is the

25 ability to have the cipher algorithm defined after the manufacture of the hardware which will carry out the algorithm. The preferred embodiment shown in Figure 1 accomplishes this goal by the use of electronically erasable, programmable array logic devices and random

30 access memory. After the manufacture of the encryption device 10 and its insertion into the communications equipment, an external device such as a microprocessor controlled computer is coupled to the address and data bus ports and is utilized to program the internal gate

35 configurations of each EEPAL with a test algorithm and define initial test data stored in RAM 32. After testing is complete the communications equipment can be delivered

to the customer with the test program still in the
encryption device so that the completed unit can be
handled without the use of security measures. The
customer would then load the encryption device with the
5   cipher algorithm by use of a similar external computer.
        Since the cipher algorithm can not be determined
based on the test algorithm, it is not necessary to have
strict security control of such equipment prior to the
actual cipher algorithm being externally programmed.
10   This permits the encryption hardware as well as equipment
containing the hardware to be manufactured without a
strict security control environment.
        In order to better understand the operation of the
encryption apparatus 10, the following illustrative
15   example is provided. An external computer which has been
preprogrammed to define the EEPAL's and load initial data
into RAM is coupled to the address and data bus. The
EEPAL's are each sequentially programmed to perform a
specific Boolean algebra function. A key and
20   initialization data are stored in RAM 32. The apparatus
is now ready to process incoming data on input 54 since
it contains the desired cipher algorithm.
        The first input data byte or word is stored in RAM
32. The key and the input data stored in RAM 32 are
25   transferred as input data to EEPAL 34 which acts upon
such data to produce a resulting output data R1. The
resulting data R1 is stored in RAM 32. The
initialization data and the resulting data R1 are
transferred from RAM 32 to EEPAL 36 which acts upon these
30   inputs to produce output data F. This output data F is
stored in RAM 32 and is substituted in the place of the
initialization data so that it will be used in the place
of same for the next input data to be encrypted.
Simultaneously, the data F is transferred to latch 26 and
35   is clocked out at line 52 as the encrypted output data.
A repetitive process occurs for each new input data byte
to produce a corresponding output encrypted data.

The above example illustrates a possible encryption application. It will be apparent that since RAM 32 is available, intermediate products can be stored and later used for subsequent calculations in a variety of ways
5   depending upon the complexity of the mathematical functions used. Depending upon the level of security desired, the number of iterations required, and the speed at, which the encryption processed must occur, more or fewer EEPAL's can be used.

10   Another advantage of the present invention resides in the use of the RAM 32 instead of an alternative storage device such as a shift register. The RAM can function as a programmable register thereby allowing the number of bytes which can be stored during any process to
15   be varied within the ultimate capacity of the RAM. This adds a degree of security to such an apparatus since it increases the difficulty of determining the number of bytes or length of the calculations being used.

The encryption apparatus of the present invention
20   can also be contrasted with the use of a general purpose microprocessor or a more specialized digital signalling processor to accomplish a similar encryption technique. Although such alternatives could be used, the relatively complicated internal structure of the microprocessor
25   makes such an alternative difficult to design to "fail safe"; that is, fail in an acceptable manner which protects the security of the message without compromising the algorithm being utilized. The more direct functioning apparatus in accordance with the present
30   invention can be more easily protected and diagnosed in the event of a failure.

Figure 2 illustrates communication equipment consisting of a two-way radio which incorporates the encryption apparatus 10 in accordance with the present
35   invention. An antenna 60 couples signals carrying voice information to a duplexer and filter 62 which couples a received signal to mixer 64. The other signal to mixer

64 from oscillator 66 is mixed to produce a resulting
intermediate frequency output 68. Conventional receiver
circuits between 68 and demodulator 70 are not shown.
The demodulator provides an output to multiplexer 72
5   which routes the received encrypted signal as digital
input 54 to the encryption device 10. The decrypted
output 52 from the device 10 is coupled by multiplexer 74
to digital to analog converter 76. The analog output
from converter 76 is amplified by audio amplifier 78
10 before being coupled to speaker 80.

The signal received will have been encrypted by a
corresponding encryption device 10 in a remote radio
utilizing a corresponding cipher algorithm and key. In
this example the recovered data is decrypted by device 10
15 and converted to an analog signal to provide a clear text
voice message to the listener.

To transmit an encrypted message, a voice signal is
coupled by microphone 82 to audio amplifier 84 whose
output is converted into a digital signal by analog to
20 digital converter 86. The output of this converter is
coupled by multiplexer 72 to encryption device 10 which
encrypts the input data and provides an output 52 coupled
by multiplexer 74 to the modulator 88 in a transmitter.
The conventional transmitter stages normally found
25 between modulator 88 and power amplifier 90 are not
shown. The amplified signal from amplifier 90 is coupled
through filter 62 to antenna 60 where it is transmitted
to a corresponding receiver having a similar encryption
device 10.

30 As previously explained, the manufacture of such a
radio would require security and accounting procedures if
the encryption device 10 contained the cipher algorithm
during the manufacture of the radio. Since the present
invention allows the cipher algorithm to be loaded at a
35 later time, the radio including the encryption device 10
can now be manufactured in a factory environment not
subject to strict security measures.

Although a radio transceiver is shown in Figure 2 as
incorporating the encryption device, it will be apparent
that other communications equipment designed to carry
voice or data, such as modems and secure telephones can
5   equally use the encryption apparatus according to the
present invention.

Although an embodiment of the present invention has
been described and illustrated herein, the scope of the
invention is defined by the claims which follow.
10

15

20

25

30

35

What is claimed is:

1.   A cryptographic apparatus for encrypting and
decrypting digital words comprising:

5   means for electronically storing a cipher algorithm,
said storing means having at least one electrically
programmable array logic device containing a portion of
said algorithm and at least one random access memory
device coupled to said logic device for storing digital
10   data generated by said algorithm; and
         means coupled to said logic device and memory device
for controlling the execution of said algorithm for each
of said digital words thereby decrypting encrypted
digital words and encrypting non-encrypted digital words.
15

20

25

30

35

- 10 -

2.   The cryptographic apparatus according to claim 1 wherein said logic device is erasable.

3.   The cryptographic apparatus according to claim 2 wherein said logic device is electrically

5   erasable.

4.   The cryptographic apparatus according to claim 1 wherein said controlling means comprises another electrically programmable array logic device.

5.   The cryptographic apparatus according to

10   claim 1 further comprising common digital address and data buses coupled to said array logic device, memory device and said controlling means, said address and data buses each having a communication port that allows said array logic device, memory device, and controlling means

15   to be programmed by an external programming device to execute the cipher algorithm.

6.   The cryptographic apparatus according to claim 4 further comprising common digital address and data buses coupled to said one array logic device,

20   another array logic device, memory device and said controlling means, said address and data buses each having a communication port that allows said one logic device, another logic device, memory device, and controlling means to be programmed by an external

25   programming device to execute the cipher algorithm.

7.   The cryptographic apparatus according to claim 1 wherein said controlling means does not include a microprocessor.

30

35

- 11 -

    8.   A two-way communication device comprising:
        means for demodulating received encrypted signals to
provide inbound encrypted digital words;
        means for generating modulated signals corresponding
5   to outbound encrypted digital words;
        cryptographic means for decrypting said inbound
encrypted digital words and generating said outbound
encrypted digital words from non-encrypted digital words,
said cryptographic means comprising:
10   means for electronically storing a cipher
algorithm, said storing means having at least one
electrically programmable array logic device containing a
portion of said algorithm and at least one random access
memory device coupled to said logic device for storing
15 digital data generated by said algorithm; and
                means coupled to said logic device and
memory device for controlling the execution of said
algorithm for decrypting said inbound encrypted digital
words and generating said outbound encrypted digital
20 words based on non-encrypted digital words.

25

30

35

- 12 -

9.   The communication device according to claim 8 wherein said logic device is erasable.

10.   The communication device according to claim 9 wherein said logic device is electrically erasable.

5   11.   The communication device according to claim 8 wherein said controlling means comprises another electrically programmable array logic device.

12.   The communication device according to claim 8 further comprising common digital address and data 10 buses coupled to said array logic device, memory device and said controlling means, said address and data buses each having a communication port that allows said array logic device, memory device, and controlling means to be programmed by an external programming device to execute 15 the cipher algorithm.

13.   The communication device according to claim 11 further comprising common digital address and data buses coupled to said one array logic device, another array logic device, memory device and said controlling 20 means, said address and data buses each having a communication port that allows said one array logic device, another array logic device, memory device, and controlling means to be programmed by an external programming device to execute the cipher algorithm.

25   14.   The communication device according to claim 8 wherein said controlling means does not include a microprocessor.

15.   The communication device according to claim 8 in which said device comprises a two-way wireless radio 30 transceiver including a receiver which receives said encrypted signals and a transmitter which transmits said modulated signals.

35

16. A method for manufacturing a communication
device which includes a cryptographic apparatus
comprising the steps of:

installing said cryptographic apparatus in said
5   communication device, said cryptographic apparatus not
including at the time of installation the cipher
algorithm to be used;

loading said cryptographic apparatus with a test
algorithm that allows it to be tested;

10   testing said communication device and cryptographic
apparatus for proper operation; and

following said installation and testing, erasing the
test algorithm and electronically redefining the
interconnection of logic gates within said cryptographic
15 apparatus to perform a Boolean algebraic function that
forms part of the cipher algorithm to be used, whereby
the communication device and cryptographic apparatus do
not substantially compromise the security of the cipher
algorithm prior to the definition of the Boolean
20· algebraic function.

25

30

35

17. The method according to claim 16 wherein said step of erasing comprises electronically erasing the test algorithm.

18. The method according to claim 16 further
5 comprising the step of electronically programming an erasable, programmable array logic device to include said Boolean algebraic function.

19. The method according to claim 16 further comprising the step of loading the cipher algorithm into
10 said cryptographic apparatus over common digital address and data buses contained within the cryptographic apparatus, said Boolean algebraic function being electronically defined in an erasable, programmable array logic device coupled to said buses within said
15 cryptographic apparatus.

20

25

30

35

FIG. 1
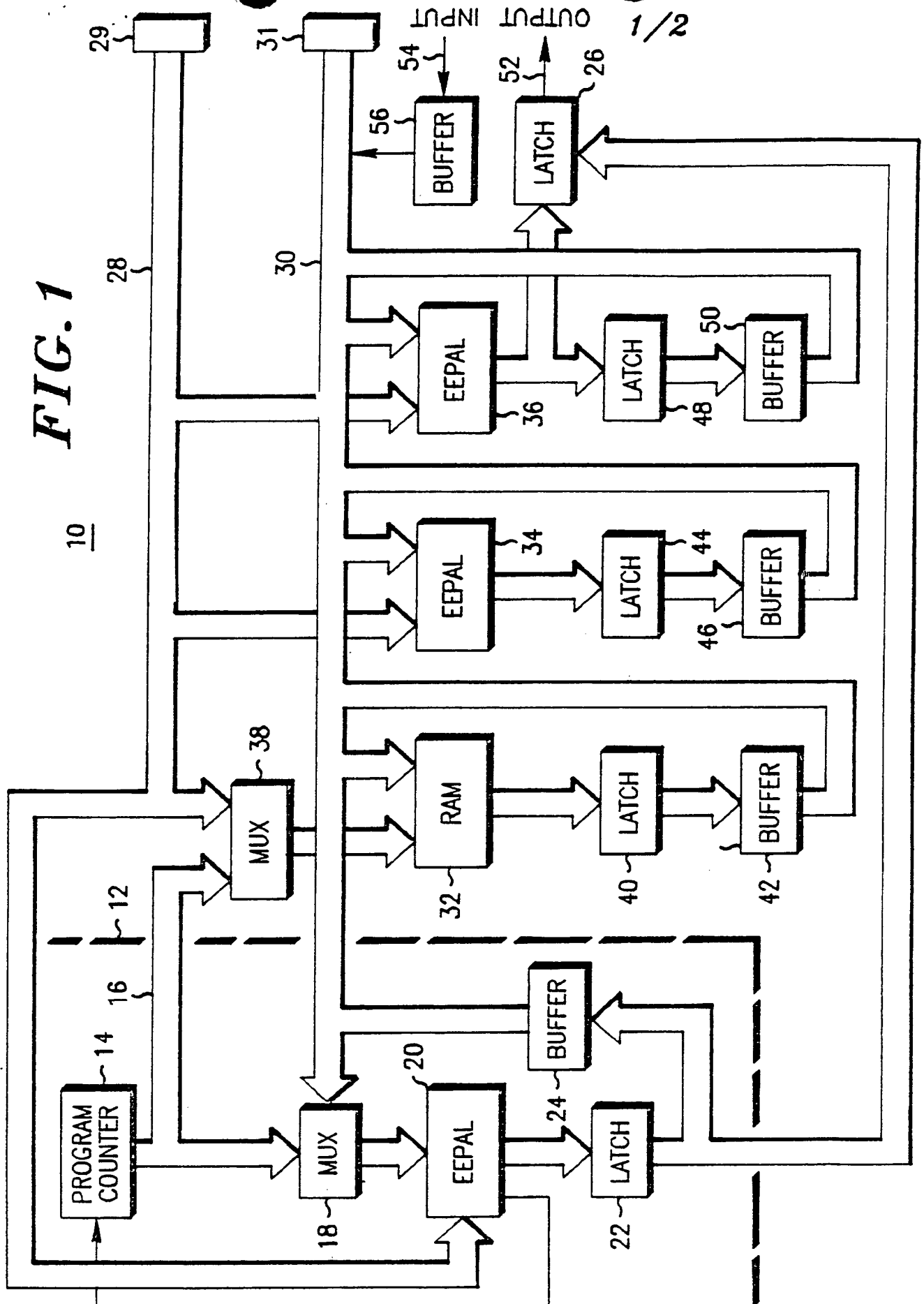
2/2

FIG.2
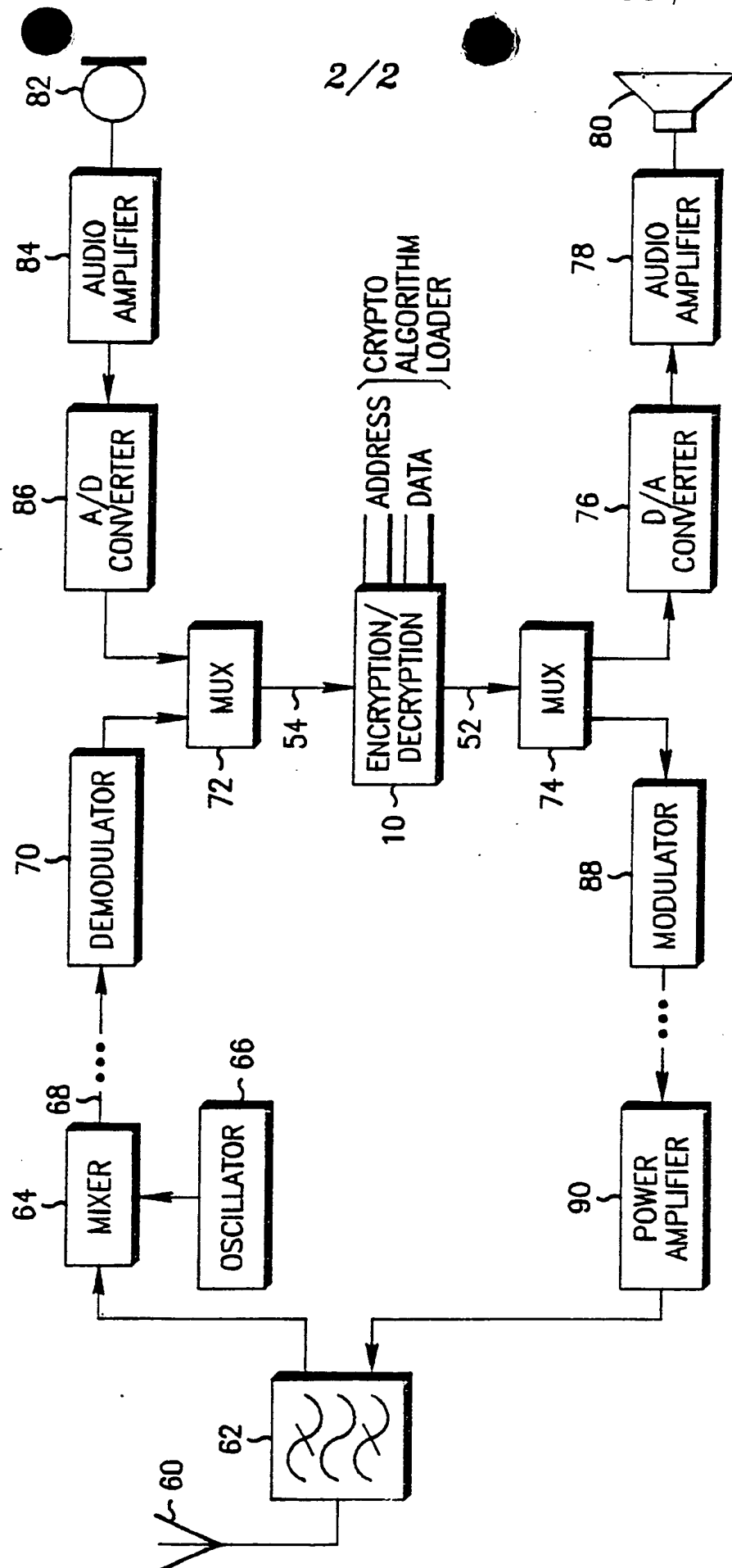
INTERNATIONAL SEARCH REPORT

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) 6

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(4) HO4K 1/00   U.S.Cl.   380/9, 28, 29, 49, 50

II. FIELDS SEARCHED

Minimum Documentation Searched 7	
Classification System	Classification Symbols
U.S.	380/9,28,29,49,50

Documentation Searched other than Minimum Documentation
to the Extent that such Documents are Included in the Fields Searched 8

III. DOCUMENTS CONSIDERED TO BE RELEVANT 9

Category *	Citation of Document, 11 with indication, where appropriate, of the relevant passages 12	Relevant to Claim No. 13
Y	US, A, 4,004,089 (RICHARD et al) 18 JANUARY 1977 See Figure 1.	1-19
Y	US, A, 4,274,085 (MARINO, JR) 16 JUNE 1981 See Cols. 8 and 9.	1-19
A	US, A, 4,306,289 (LUMLEY), 15 DECEMBER 1981 See entire Document.	1-19
Y	US, A, 4,484,025 (OSTERMANN et al) 20 NOVEMBER 1984 See Figure 2.	1-19
Y	US, A, 4,598,170 (PIOSENKA et al) 1 JULY 1986 See Figure 7.	1-19
Y	US, A, 4,747,139 (TAAFFE) 24 MAY 1988 See Col. 3, lines 50-60.	1-19

* Special categories of cited documents: 10

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
08 MARCH 1989	0 4 MAY 1989

International Searching Authority	Signature of Authorized Officer
ISA/US	Salvatore Cangialosi

Form PCT/ISA/210 (second sheet) (Rev.11-87)

THIS PAGE BLANK (USPTO)